



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,321	03/02/2004	Christopher N. Kline	END920030127US1	1828
68786	7590	07/09/2008	EXAMINER	
CHRISTOPHER & WEISBERG, P.A. 200 EAST LAS OLAS BOULEVARD SUITE 2040 FORT LAUDERDALE, FL 33301			TABOR, AMARE F	
		ART UNIT	PAPER NUMBER	
		2139		
		MAIL DATE		DELIVERY MODE
		07/09/2008		PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/791,321	KLINE, CHRISTOPHER N.	
	Examiner	Art Unit	
	AMARE TABOR	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 09 May 2008.
 2a) This action is **FINAL**. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-14, 16 and 17 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-14, 16 and 17 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 02 March 2004 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ . |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____. | 6) <input type="checkbox"/> Other: _____ . |

DETAILED ACTION

1. This correspondence is in response to **Amendments** and **REMARKS** filed on May 09, 2008.
2. Claims 1, 3-11, 13-14 and 16-17 are amended; And Claim 15 is cancelled.
3. Claims 1-14, 16 and 17 are pending.

Response to Arguments

4. Applicant's arguments filed on 05/09/2008 have been fully considered but they are not persuasive.

Regarding AAPA in view of Ashland

Applicant argued:

*"...the procedures referenced in AAPA do not involve comparing to a **list of individuals**, nor do they involve determining if a group with privilege level higher than user level is on a **list of group names** generally used for a group with user level privilege. The procedures in AAPA rely exclusively on the general knowledge of the system administrator. There is no mention of any type of list being referenced at all..."*

Additionally, Applicant argued:

*"...Ashland teaches a method and system for controlling access system resources by **assigning privilege levels to different groups of users**, but it does not teach a method for determining that previously assigned privilege levels are improper..."*

Examiner respectfully disagrees.

First, as indicated in the prior office action, AAPA discloses that "...it was previously known for a system administrator to periodically, manually enter commands into the computer to output the group names and their privilege levels to a text file..." [p.2, lines 16-18]; therefore, the invention proposes a computer program product to "...identify and adjust any groups whose privilege levels may be too high"

[p.3, lines 4-5]. Furthermore, AAPA discloses "...*[t]his manual process was time consuming when a large number of computers were checked...*" [p.2, lines 21-22 and 29]. In other words, the invention address the deficiencies of the prior art [system administrator manually identifying and adjusting group levels] by simply automating the process.

Second, Applicant's argument AAPA not disclosing "list of individuals" or "list of group names" in the amended claims is not persuasive. AAPA discloses administrators periodically determine privilege levels by reviewing privilege levels of group names [and members of a group]. AAPA discloses that the administrator do this determination through 'personal knowledge', which obviously indicates that the administrator keeps an updated record for group and member privilege levels. It may be argued that AAPA does not specifically disclose system administrator keeping an updated record; however, Ashland discloses "list of group names" [see GROUPS – GROUP 1, GROUP 2,... GROUP N in FIG.4] and "list of individuals" in each group [see USERID 1, USERID 2,... USER ID 6 in FIG.4].

Third, abstract of Ashland begins by stating "*An improved system and method is provided for managing system-level privileges and for...*" Therefore, the combination of AAPA and Ashland obviously disclose the claimed invention.

Regarding Kuhn in view of Clark

Applicant argued:

"...*Kuhn does not disclose a method for determining whether a group has been improperly assigned a privilege level higher than user level privilege ... Kuhn discloses verifying that a subject has a privilege if the subject has been selected or assigned and active role. In contrast, the claimed feature recites determining whether a group that has a privilege level **higher** than user level privilege actually has a group name on the list of group names generally used for a group with **user** level privilege ...*"

Examiner respectfully disagrees. As indicated in the prior office action, Kuhn discloses a role based access control (RBAC) system. Specifically, Kuhn discloses four equations that disclosed the

claimed features of the invention [see col.5, lines 34 to col.6, line 46]. For example, Kuhn discloses “*...Eq.(1) states, in effect, that human users are authorized to execute privilege assigned to a role only if they belong to the class of subjects authorized for that role...*” In other words, Equation (1) ensures [or determines] if a user [or member] is [or is not] in the class of subjects [or list of individuals] authorized [or trusted] for that role. Additionally, Kuhn discloses, “*...Equation (4) refers to privilege authorization: a subject can execute a privilege only if the privilege is authorized for a role in which the subject is currently active...*” In other words, Equation (4) determines privilege of a subject [or member] based on his/her authorization status for a role. Equations (2) and (3) disclose role assignment and authorization; i.e., group level assignment and privilege determination.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 3, 6, 8 and 11 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- The claims recite, “*...the members of the group are revealed as potentially not trusted*”; however, the phrase “**potentially not trusted**” renders the claim indefinite.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-14, 16 and 17 rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant's Admitted Prior ART ("AAPA") in view of Ashland et al. (US 7,219,234 B1, referred as "Ashland")

As per Claim 1, AAPA discloses,

first program instructions to compare each members within the group to a first list, the first list including names of trusted individuals [p.2, lines 26-28];

second program instructions to determine whether the groups includes at least one member not on the first list and if so, generate a report identifying said at least one member not on the first list and the group in which said at least one member is a member [p.2, lines 18-20 – *where AAPA discloses system administrator identifying the unprivileged member*]; and

third program instructions to determine whether the group has a group name on a second list, the second list including group names generally used for a group with user level privilege, and if so, generate a report indicating that the group has a group name generally used for a group having user level privilege, such that members of the group are revealed as potentially not trusted [p.2, lines 16-18 – *where AAPA discloses system administrator identifying the unprivileged group*].

AAPA discloses administrators periodically determine privilege levels by reviewing privilege levels of group names [and members of a group]; but does not explicitly disclose first and second list of trusted individuals and group names, and

a computer program product, recorded a computer readable medium, for determining that a group has been improperly assigned a privilege level higher than user level privilege, the group including a plurality of members.

However, Ashland discloses first and second list of trusted individuals [see **USERID 1, USERID 2,... USER ID 6** in FIG.4] and group names [see **GROUPS – GROUP 1, GROUP 2,... GROUP N** in FIG.4], and

a computer program product, recorded a computer readable medium [see FIGS. 1, 2, 4 and 5], for determining that a group has been improperly assigned a privilege level higher than user level privilege, the group including a plurality of members [abstract].

Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify AAPA by including the computer program product recorded on a computer readable medium of Ashland. The modification automates the manual system of checking privilege level of groups and members done by the system administrator. Furthermore, the modification will increase the efficiency of the manual checking system and decrease the overall overhead [see BACKGROUND OF THE INVENTION of AAPA].

As per Claim 6, AAPA discloses,

means for comparing members within the group to a first list, the first list including names of trusted individuals [p.2, lines 26-28];

means for determining whether the group includes at least one member not on the first list, and if so, generating a report identifying the at least one member and the group in which said the at least one member is included [p.2, lines 18-20 – *where AAPA discloses system administrator identifying the unprivileged member*]; and

means for determining whether the group has a group name on a second list, the second list including group names generally used for a group with user level privilege, and if so, generating a report indicating that the group has a group name generally used for a group with user level privilege, such that the members of the group are revealed as potentially not trusted [p.2, lines 16-18 – *where AAPA discloses system administrator identifying the unprivileged group*].

AAPA discloses administrators periodically determine privilege levels by reviewing privilege levels of group names [and members of a group]; but does not explicitly disclose first and second list of trusted individuals and group names, and a computer system for determining that a group has been improperly assigned a privilege level higher than user level privilege, the group including a plurality of members.

However, Ashland discloses first and second list of trusted individuals [see **USERID 1, USERID 2,... USER ID 6** in FIG.4] and group names [see **GROUPS – GROUP 1, GROUP 2,... GROUP N** in FIG.4], and a computer system [see FIGS. 1, 2, 4 and 5] for determining that a group has been improperly assigned a privilege level higher than user level privilege, the group including a plurality of members [abstract].

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify AAPA by including the computer system of Ashland. The modification automates the manual system of checking privilege level of groups and members done by the system administrator. Furthermore, the modification will increase the efficiency of the manual checking system and decrease the overall overhead [see BACKGROUND OF THE INVENTION of AAPA].

As per Claim 11, AAPA discloses,

first program instructions to compare each members within the group to a first list, the first list including names of trusted individuals [p.2, lines 26-28];

second program instructions to determine whether the .groups includes at least one member not on the first list, and if so, generate a report identifying said at least one member not on the first list and the group in which said at least one member is a member [p.2, lines 18-20]; and

third program instructions to determine whether the group has a group name not on a second list, the second list including group names generally used for a group having a privilege level higher than user level privilege, and if so, generate a report indicating that the group has a group name not generally used for a group having a privilege level higher than user level privilege, such that the members of the group are revealed as potentially not trusted [p.2, lines 16-18].

AAPA discloses administrators periodically determine privilege levels by reviewing privilege levels of group names [and members of a group]; but does not explicitly disclose first and second list of trusted individuals and group names, and a computer system, recorded a computer readable medium, for determining that a group has been improperly assigned a privilege level higher than user level privilege.

However, Ashland discloses first and second list of trusted individuals [see **USERID 1, USERID 2,... USER ID 6** in FIG.4] and group names [see **GROUPS – GROUP 1, GROUP 2,... GROUP N** in FIG.4], and a computer system, recorded a computer readable medium [see FIGS. 1, 2, 4 and 5], for determining that a group has been improperly assigned a privilege level higher than user level privilege [abstract].

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify AAPA by including the computer program product recorded on a computer readable medium of Ashland. The modification automates the manual system of checking privilege level of groups and members done by the system administrator. Furthermore, the modification will increase the efficiency of the manual checking system and decrease the overall overhead [see BACKGROUND OF THE INVENTION of **AAPA**].

As per Claim 16, AAPA discloses,

first program instructions to determine that a group with an actual privilege level higher than user level privilege has a group name on a list of group names generally used for a group with user level privilege; and second program instructions, responsive to a determination of a group with an actual privilege level higher than user level privilege with a group name generally used for a group with a privilege level no higher than user level privilege, to compare members of said group to a list of trusted individuals [p.2, lines 18-20 and 26-28], and

if any member said group does not appear on said list of trusted individuals, remove said member from said group [p.2, lines 20-21].

AAPA discloses administrators periodically determine privilege levels by reviewing privilege levels of group names [and members of a group]; but does not explicitly disclose first and second list of trusted individuals and group names, and a computer program product, recorded in a computer readable medium, for managing privileges of groups; however, Ashland discloses first and second list of trusted individuals [see **USERID 1, USERID 2,... USER ID 6** in FIG.4] and group names [see **GROUPS –**

GROUP 1, GROUP 2,... GROUP N in FIG.4], and a computer program product [see FIGS. 1, 2, 4 and 5], recorded in a computer readable medium, for managing privileges of groups [abstract].

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify AAPA by including the computer program product recorded on a computer readable medium of Ashland. The modification automates the manual system of checking privilege level of groups and members done by the system administrator. Furthermore, the modification will increase the efficiency of the manual checking system and decrease the overall overhead [see BACKGROUND OF THE INVENTION of AAPA].

As per Claim 17, AAPA discloses,

first program instructions to determine that a group with an actual privilege level higher than user level privilege has a group name not on a list of group names generally used for a group with privilege level higher than user level privilege; and second program instructions, responsive to a determination of a group with an actual privilege level higher than user level privilege with a group name not generally used for a group with privilege level higher than user level privilege, to compare members of said group to a list of trusted individuals [p.2, lines 18-20 and 26-28], and

if any member said group does not appear on said list of trusted individuals, lower the actual privilege level of said group [p.2, lines 20-21 – *where AAPA discloses system administrator lowering privilege of a group depending on the outcome of the investigation*].

AAPA discloses administrators periodically determine privilege levels by reviewing privilege levels of group names [and members of a group]; but does not explicitly disclose first and second list of trusted individuals and group names, and a computer program product, recorded in a computer readable medium, for managing privileges of groups; however, Ashland discloses first and second list of trusted individuals [see **USERID 1, USERID 2,... USER ID 6** in FIG.4] and group names [see **GROUPS – GROUP 1, GROUP 2,... GROUP N** in FIG.4], and a computer program product, recorded in a computer readable medium, for managing privileges of groups [see FIGS.1, 2, 4 and 5 and abstract].

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify AAPA by including the computer program product recorded on a computer readable medium of Ashland. The modification automates the manual system of checking privilege level of groups and members done by the system administrator. Furthermore, the modification will increase the efficiency of the manual checking system and decrease the overall overhead [see BACKGROUND OF THE INVENTION of **AAPA**].

As per Claim 2, AAPA-Ashland combination discloses,

wherein there are a plurality of applications or application instances, and a same group can be assigned different privilege levels for involvement with different applications or application instances [see FIGS.4-6 – where **Ashland** discloses assigning different privilege levels to members in a group]; said third program instructions makes its determination separately for each application or application instance [see step 704 in FIG.7 of **Ashland**]; and

means for determining whether the group has a group name generally used for a group with user level privilege makes its determination for each application or application instance [see **administrator** in **AAPA**] .

Claims 7 and 12 are rejected for the same reasons applied to the rejection of Claim 2.

As per Claim 3, AAPA-Ashland combination discloses,

fourth program instructions and means to determine whether the group has a group name not included on a third list, the third list including group names generally used for a group having a privilege level higher than user level privilege [see p.2, lines 18-20 and 26-28 of **AAPA**],

and if so, generate a report indicating that the group has a group name not on the third list, such that members of the group are revealed as potentially not trusted [see p.2, lines 16-18 of **AAPA**]; and

wherein said fourth program instructions are recorded on said medium [see abstract, FIGS.1, 2, 4 and 5 of **Ashland**].

Claim 8 is rejected for the same reasons applied to the rejection of Claim 3.

As per Claim 4, AAPA-Ashland combination discloses,
wherein said second program instructions and means to determine whether the group includes at least one members not on the first list [see p.2, lines 18-20 and 26-28 of **AAPA**],
and if so not, generate a report indicating that the group has all its members on the first list [see p.2, lines 16-18 of **AAPA**].

Claims 9 and 13 are rejected for the same reasons applied to the rejection of Claim 4.

As per Claim 5, AAPA-Ashland combination discloses,
fourth program instructions, responsive to determining that the group has a group name on the second list, and means to determine are the group is on the first list [see p.2, lines 18-20 and 26-28 of **AAPA**]; and

wherein said fourth program instructions are recorded on said medium [see abstract, FIGS.1, 2, 4 and 5 of **Ashland**].

Claims 10 and 14 are rejected for the same reasons applied to the rejection of Claim 5.

Claims 1-14 and 16 rejected under 35 U.S.C. 103(a) as being unpatentable over “Kuhn” (US 6,023,765) in view of Clark et al. (US 7,237,119 B2, referred as “Clark”)

As per Claim 1, KUHN discloses,
A computer program product, recorded a computer readable medium, for determining that a group has been improperly assigned a privilege level higher than user level privilege, the group including a plurality of members, said computer program product [see col.1, lines 12 and 13] comprising:
first program instructions to compare each members within the group to a first list, the first list including names of trusted individuals [see for example, col.1, lines 23-29];

second program instructions to determine whether the groups includes at least one member not on the first list [see **Equations (1) and (4)** in col.6; and for example, col.5, lines 65-67]; and

third program instructions to determine whether the group has a group name on a second list, the second list including group names generally used for a group with user level privilege [see **Equations (2) and (3)** in col.6; for example, col.6, lines 7-15].

Kuhn does not explicitly disclose generate a report identifying said at least one member not on the first list and the group in which said at least one member is a member, and generate a report indicating that the group has a group name generally used for a group having user level privilege, such that members of the group are revealed as potentially not trusted.

However, in the same field of endeavor, Clark discloses generating a report identifying said at least one member not on the first list and the group in which said at least one member is a member, and generating a report indicating that the group has a group name generally used for a group having user level privilege, such that members of the group are revealed as potentially not trusted [see FIGS.3-5 and 7; and for example, col.3, line 37 to col.14].

Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to combine the teachings of Kuhn and Clark because both are in the fields of managing user authorization levels. Incorporating Clark's teaching modifies the teachings of Kuhn to generate a report on the current status of members and group names, because Kuhn's system is implemented on an MLS system by establishing a mapping between privileges within the RBAC system and pairs of levels and sets of compartments assigned to objects within the MLS system. Furthermore, in Kuhn each user's request for a privilege is checked to ensure that it is permitted to the subject's role at the time of the request; and therefore, Kuhn's system could be modified to generate a report using the user interface of Clark whenever the said mapping process is performed [see abstract; and SUMMARY OF INVENTION in col.3 of **Kuhn**].

As per Claim 6, KUHN discloses,

A computer system for determining that a group has been improperly assigned a privilege level higher than user level privilege, said computer system [see col.1, lines 12 and 13] comprising: the group including a plurality of members means for comparing members within the group to a first list, the first list including names of trusted individuals [see **RBAC TRUSTED INTERFACE 40** in FIG.3 and **USERS 26**, **USER ID 28** in FIG.2; and for example, col.7, line 61 to col.8, line 14 – *where Kuhn discloses authorizing users by their user ids*];

means for determining whether the group includes at least one member not on the first list [see **(ROLE, PRIVILEGE) REQUEST 46**, **RBAC TO MLS MAPPING FUNCTION 48** in FIG.3; and **Equations (1)** and **(4)** in col.6]; and

means for determining whether the group has a group name on a second list, the second list including group names generally used for a group with user level privilege [see **[COMPARTMENTS]**, **LEVEL 50** in FIG.3; and see **Equations (2)** and **(3)** in col.6].

Kuhn does not explicitly disclose generating a report identifying the at least one member and the group in which said the at least one member is included, and generating a report indicating that the group has a group name generally used for a group with user level privilege, such that the members of the group are revealed as potentially not trusted; however, Clark discloses the above repot generating mechanism [see FIGS.3-5 and 7; and for example, col.3, line 37 to col.14].

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify the system of Kuhn by incorporating Clark's teaching to generate a report on the current status of members and group names, because Kuhn's system is implemented on an MLS system by establishing a mapping between privileges within the RBAC system and pairs of levels and sets of compartments assigned to objects within the MLS system [see abstract; and SUMMARY OF INVENTION in col.3 of **Kuhn**].

As per Claim 11, KUHN discloses,

A computer system, recorded a computer readable medium, for determining that a group has been improperly assigned a privilege level higher than user level privilege first program instructions to compare each members within the group to a first list, the group including a plurality of members, said computer program product [see col.1, lines 12 and 13] comprising: the first list including names of trusted individuals [see col.1, lines 23-29];

second program instructions to determine whether the .groups includes at least one member not on the first list [see **Equations (1) and (4)** in col.6]; and

third program instructions to determine whether the group has a group name not on a second list, the second list including group names generally used for a group having a privilege level higher than user level privilege [see **Equations (2) and (3)** in col.6; and for example, col.6, lines 7-15].

Kuhn does not explicitly disclose generate a report identifying said at least one member not on the first list and the group in which said at least one member is a member, and generate a report indicating that the group has a group name not generally used for a group having a privilege level higher than user level privilege, such that the members of the group are revealed as potentially not trusted; however, Clark discloses the report generating mechanism [see FIGS.3-5 and 7; and for example, col.3, line 37 to col.14].

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify the system of Kuhn by incorporating Clark's teaching to generate a report on the current status of members and group names, because Kuhn's system is implemented on an MLS system by establishing a mapping between privileges within the RBAC system and pairs of levels and sets of compartments assigned to objects within the MLS system [see abstract; and SUMMARY OF INVENTION in col.3 of **Kuhn**].

As per Claim 16, KUHN discloses,

A computer program product, recorded in a computer readable medium, for managing privileges of groups, said computer program product [see col.1, lines 12 and 13] comprising: first program

instructions to determine that a group with an actual privilege level higher than user level privilege has a group name on a list of group names generally used for a group with user level privilege [see **Equations (2) and (3)** in col.6]; and

second program instructions, responsive to a determination of a group with an actual privilege level higher than user level privilege with a group name generally used for a group with a privilege level no higher than user level privilege, to compare members of said group to a list of trusted individuals [see **Equations (1) and (4)** in col.6; and for example, col.5, lines 65-67].

Kuhn does not explicitly disclose if any member said group does not appear on said list of trusted individuals, remove said member from said group; however, Clark discloses removing said member from said group if any member said group does not appear on said list of trusted individuals [see **Del Row** in FIGS.4 and 7; **Level 140** in FIG.4; and for example, col.3, line 46 to col.4, line 23].

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify the system of Kuhn by incorporating Clark's teaching to remove members from list, because Kuhn's system is implemented on an MLS system by establishing a mapping between privileges within the RBAC system and pairs of levels and sets of compartments assigned to objects within the MLS system [see abstract; and SUMMARY OF INVENTION in col.3 of **Kuhn**].

As per Claim 2, KUHN-Clark combination discloses,

wherein there are a plurality of applications or application instances, and a same group can be assigned different privilege levels for involvement with different applications or application instances [see FIGSROLES 30, OPERATIONS 32 in FIG.3; and see also FIGS.5 and 6 of **Kuhn**]; said third program instructions makes its determination separately for each application or application instance [see **PRIVILEGE SETS, PRIVILEGE SET, ROLE COMARTMENT LABELS** in FIG.6 of **Kuhn**]; and

means for determining whether the group has a group name generally used for a group with user level privilege makes its determination for each application or application instance [see **RBAC TO MLS MAPPING FUNCTION 48** in FIG.3 of **Kuhn**].

Claims 7 and 12 are rejected for the same reasons applied to the rejection of Claim 2.

As per Claim 3, KUHN-Clark combination discloses,

fourth program instructions and means to determine whether the group has a group name not included on a third list [see FIG.5 and **PRIVILEGE SETS, PRIVILEGE SET, ROLE COMARTMENT LABELS** in FIG.6 of **Kuhn**], the third list including group names generally used for a group having a privilege level higher than user level privilege [see **RBAC TO MLS MAPPING FUNCTION 48** in FIG.3 of **Kuhn**],

and if so, generate a report indicating that the group has a group name not on a the third list, such that members of the group are revealed as potentially not trusted [see FIGS.3-5 and 7; and for example, col.3, line 37 to col.14 of **Clark**; and

wherein said fourth program instructions are recorded on said medium [see FIG.1 of **Clark**; and col.1, lines 12 and 13 of **Kuhn**].

Claim 8 is rejected for the same reasons applied to the rejection of Claim 3.

As per Claim 4, KUHN-Clark combination discloses,

wherein said second program instructions and means to determine whether the group includes at least one members not on the first list [see **RBAC TO MLS MAPPING FUNCTION 48** in FIG.3; and for example, col.5, line 35 to col.7, line 60 of **KUHN**],

and if so not, generate a report indicating that the group has all its members on the first list [see FIGS.3-5 and 7; and for example, col.3, line 37 to col.14 of **Clark**].

Claims 9 and 13 are rejected for the same reasons applied to the rejection of Claim 4.

As per Claim 5, KUHN-Clark combination discloses,

fourth program instructions, responsive to determining that the group has a group name on the second list, and means to determine are the group is on the first list [see **RBAC TO MLS MAPPING FUNCTION 48** in FIG.3; and for example, col.5, line 35 to col.7, line 60 of **KUHN**]; and

wherein said fourth program instructions are recorded on said medium [see FIG.1 of **Clark**; and col.1, lines 12 and 13 of **Kuhn**].

Claims 10 and 14 are rejected for the same reasons applied to the rejection of Claim 5.

Claim 17 rejected under 35 U.S.C. 103(a) as being unpatentable over “Kuhn” in view of Morris et al. (EP 1 112 184 A2, referred as “Morris”)

As per Claim 17, KUHN discloses,

A computer program product, recorded in a computer readable medium, for managing privileges of groups, said computer program product [see col.1, lines 12 and 13 of **Kuhn**] comprising: first program instructions to determine that a group with an actual privilege level higher than user level privilege has a group name not on a list of group names generally used for a group with privilege level higher than user level privilege [see **Equations (2)** and **(3)** in col.6]; and

second program instructions, responsive to a determination of a group with an actual privilege level higher than user level privilege with a group name not generally used for a group with privilege level higher than user level privilege [see **Equations (1)** and **(4)** in col.6], to compare members of said group to a list of trusted individuals [see for example, col.1, lines 12 and 13].

Kuhn does not explicitly disclose if any member said group does not appear on said list of trusted individuals, lower the actual privilege level of said group; however, in the same field of endeavor, Morris discloses lowering the actual privilege level of said group if any member said group does not appear on said list of trusted individuals [see FIG.1 and abstract].

It would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify the system of Kuhn by incorporating Morris's teaching to lowering privilege level of a group, because Kuhn's system is implemented on an MLS system by establishing a mapping between privileges within the RBAC system and pairs of levels and sets of compartments assigned to objects within the MLS system [see abstract; and SUMMARY OF INVENTION in col.3 of **Kuhn**].

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AMARE TABOR whose telephone number is (571)270-3155. The examiner can normally be reached on Mon-Fri 8:00a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Amare Tabor
(AU 2139)

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139